On Valuation Rings

Rodney Coleman, Laurent Zwald

On Valuation Rings

Rodney Coleman* Laurent Zwald†

August 30, 2019

Abstract

Valuation rings occur in a wide variety of situations. In this paper we bring together many basic results concerning this important class of rings. In particular, we consider the relation between valuation rings and Dedekind domains.

A nonzero subring V of a field F is a *valuation ring* of F if, for every $\alpha \in F^*$, the nonzero elements of F, either $\alpha \in V$ or $\alpha^{-1} \in V$. Clearly, the field F is itself a valuation ring.

Examples

- If p is a prime number, then the set $V = \{\frac{p^r m}{n} : r \geq 0, p \not| m, p \not| n\}$ is a valuation ring of $\mathbf{Q}$.
- If F is a field, then the set $V = \{\frac{f}{g} \in F(X) : \deg f \leq \deg g\}$ is a valuation ring of $F(X)$.

We begin our study of valuation rings with some elementary properties. As a valuation ring is a subring of a field, it is commutative and an integral domain.

Proposition 1 *Let V be a valuation ring of the field F. Then*

- **a.** *The fraction field of V is F;*
- **b.** *V is a local ring, i.e., V has a unique maximal ideal;*
- **c.** *V is integrally closed in F;*
- **d.** *Any subring of F containing V is also a valuation ring.*

PROOF **a.** Clearly the fraction field of V is contained in F. On the other hand, if $\alpha \in F^*$, then we may write $\alpha = \frac{\alpha}{1}$ or $\alpha = \frac{1}{\alpha^{-1}}$. As α or $\alpha^{-1} \in V$, α lies in the fraction field of V.

b. It is sufficient to show that the set M of nonunits of V form an ideal. If a and b are nonzero nonunits, then $\frac{a}{b}$ or $\frac{b}{a}$ belongs to V. Suppose that $a + b$ is a unit u. If $\frac{a}{b} \in V$, then $b(1 + \frac{a}{b}) \in V$ and $b(1 + \frac{a}{b})u^{-1} = 1$, so b is a unit, a contradiction. An analogous argument applies if $\frac{b}{a}$ belongs to V. Therefore $a + b$ is a nonunit. Thus the sum of two elements of M belongs to M.

*Email: rodney.coleman@univ-grenoble-alpes.fr Laboratoire Jean Kuntzmann, Université Grenoble Alpes(UGA) 38041 Grenoble cedex 9, France.

†Email: laurent.zwald@univ-grenoble-alpes.fr Laboratoire Jean Kuntzmann, Université Grenoble Alpes(UGA) 38041 Grenoble cedex 9, France.

Suppose now that $r \in V$ and $a \in M$. We claim that $ra \in M$. If ra is a unit u, then $ru^{-1}a = 1$, which implies that a is a unit, a contradiction. Hence scalar products of elements in M belong to M. We have shown that M is an ideal in V.

c. Let $\alpha \in F^*$ be integral over V. Then there is an equation of the form

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} + \alpha^n = 0,$$

where the c_i belong to V. We must show that $\alpha \in V$. If this is not the case, then multiplying the above equation by $\alpha^{-(n-1)}$, we obtain

$$\alpha = -c_{n-1} - c_{n-2}\alpha^{-1} - \cdots - c_1\alpha^{-(n-2)} - c_0\alpha^{-(n-1)} \in V,$$

a contradiction. So $\alpha \in V$.

d. This follows directly from the definition of a valuation ring. □

Definition If M is the unique maximal ideal in the valuation ring V, then we call the field V/M the *residue field* of V.

Notation If R is a local ring, then we will sometimes write M_R for the maximal ideal in R.

In the next result we show that the ideals in a valuation ring can be ordered.

Proposition 2 *The ideals in a valuation ring V are totally ordered by inclusion. Conversely, if V is an integral domain, with fraction field F, and the ideals are ordered by inclusion, then V is a valuation ring of F.*

PROOF Suppose that I and J are ideals in V and that I is not contained in J. Then there exists $a \in I \setminus J$. If $b \in J$, we must show that $b \in I$. If $b = 0$, then we are finished, so let us suppose that this is not the case. We claim that $\frac{b}{a} \in V$. If this is not the case, then $\frac{a}{b} \in V$, which implies that $a = \frac{a}{b}b \in J$, a contradiction, so $\frac{b}{a} \in V$. Therefore $b = \frac{b}{a}a \in I$, as required.

Converse Suppose that the ideals are totally ordered in the integral domain V. If $\alpha \in F^*$, the fraction field of V, then $\alpha = \frac{a}{b}$, with $a, b \in V^*$. By hypothesis, either $(a) \subset (b)$ or $(b) \subset (a)$. Thus $a = cb$, with $c \in V$, or $b = da$, with $d \in V$. In the first case we have $\frac{a}{b} = c \in V$ and in the second case $\frac{b}{a} = d \in V$. Therefore V is a valuation ring. □

Corollary 1 *Let V be a subring of a field F. Then V is a valuation ring, if and only if, for $a, b \in V$, either a divides b or b divides a.*

PROOF Suppose that V is a valuation ring. From Proposition 2, $(a) \subset (b)$ or $(b) \subset (a)$, so $b|a$ or $a|b$.

Now suppose that for $a, b \in V$, either $a|b$ or $b|a$. If I, J are ideals in V and $I \not\subset J$, $J \not\subset I$, then there exist $a \in J \setminus I$ and $b \in I \setminus J$. If $a|b$, then $b \in J$, and if $b|a$, then $a \in I$. In both cases we have a contradiction. Hence the ideals are totally ordered by inclusion and so V is a valuation ring. □

Corollary 2 *In a valuation ring every finitely generated ideal is principal.*

PROOF Let I be an ideal in the valuation ring V and suppose that $I = (a_1, a_2, \ldots, a_n)$. Then either $a_1 \mid a_2$ or $a_2 \mid a_1$. Without loss of generality, suppose that $a_1 \mid a_2$. In this case, we have $I = (a_1, a_3, \ldots, a_n)$. Continuing in the same way, we finally obtain that $I = (a_i)$, for some i. □

We now consider the case where the valuation ring is noetherian.

Proposition 3 *If V is a noetherian valuation ring, then V is a principal ideal domain. In addition, there exists a prime element $p \in V$ such that every ideal has the form (p^m) and is thus a power of the unique maximal ideal M. In addition, for any such p, we have $\cap_{m=1}^{\infty}(p^m) = \{0\}$.*

PROOF Since V is noetherian, an ideal I is finitely generated, say by $a_1, \ldots, a_n$. From Proposition 2, we may suppose that $(a_1) \subset \cdots \subset (a_n)$. But then $I \subset (a_n) \subset I$, which implies that $I = (a_n)$. Hence V is a PID.

In particular, the maximal ideal M is (p), for some prime element p, because M is a prime ideal. Let (a) be an arbitrary ideal in V. If a is a unit, then $(a) = V$ and $(a) = (p^0)$. On the other hand, if a is a nonunit, then $a \in M$. But then $p|a$, so $a = pb$, for some $b \in V$. If b is a nonunit, then $p|b$ and we obtain $a = p^2c$, with $c \in V$. Continuing in the same way and using the fact that V is a unique factorization domain, we obtain $a = p^m u$, where u is a unit in V and m a positive integer. Thus $(a) = (p^m)$.

Finally, if $a \in (p^m)$, for all $m \geq 1$, then p^m divides a, for all $m \geq 1$. Once again using the fact that V is a UFD, we see that $a = 0$. Hence $\cap_{m=1}^{\infty}(p^m) = \{0\}$. □

Extensions of ring homomorphisms

We now aim to show how extensions of ring homomorphisms give rise to valuation rings, thus providing us with a source of such rings.

Lemma 1 *Let R be a subring of the field F, C an algebraically closed field and $h : R \longrightarrow C$ a homomorphism. If $\alpha \in F^*$, then h can be extended to a ring homomorphism $\bar{h}$ of $R[\alpha]$ into C or to a ring homomorphism $\bar{h}$ of $R[\alpha^{-1}]$ into C.*

PROOF The kernel P of h is a prime ideal of R and we may extend h to a homomorphism g of R_P, the localization at P, into C by setting

$$g(\frac{a}{b}) = \frac{h(a)}{h(b)}.$$

(Notice that $b \notin P$ implies that $h(b) \neq 0$.) We claim that the kernel of g is $R_P P$:

$$g(\frac{a}{b}) = 0 \Longrightarrow h(a) = 0 \Longrightarrow a \in P \Longrightarrow \frac{a}{b} = \frac{1}{b} \cdot a \in R_P P;$$

and

$$\frac{a}{b} \in R_P P \Longrightarrow a \in P, b \notin P \Longrightarrow g(\frac{a}{b}) = \frac{h(a)}{h(b)} = 0,$$

because $h(a) \in P$. Thus the claim is established. By the first isomorphism theorem, the image of g is isomorphic to $\frac{R_P}{R_P P}$, which is a field, because $R_P P$ is a maximal ideal in R_P. Thus g is an extension of h and $g(R_P)$ is a subfield of C. Therefore we may consider that R is a local ring and that the image of h is a subfield of C.

We extend h to a homomorphism $\tilde{h}$ of $R[X]$ into $C[X]$: If $f(X) = \sum_{i=1}^{n} a_i X^i \in R[X]$, then we set $\tilde{h}(f)(X) = \sum_{i=1}^{n} h(a_i) X^i \in C[X]$. Let $I = \{f \in R[X] : f(\alpha) = 0\}$. Then $J = \tilde{h}(I)$ is an ideal of $(\text{Im } h)[X]$, necessarily principal, because Im h is a subfield of C, and so a field. We set $J = (j(x))$. If j is nonconstant, then j has a root β in C, because C is algebraically closed. We fix β and extend h to $\bar{h} : R[\alpha] \longrightarrow C$ by setting $\bar{h}(\alpha) = \beta$.

Alternatively, suppose that j is a constant polynomial. If $j = 0$, then we may take any $\beta \in C$ and apply the argument above. On the other hand, if the constant is nonzero, then we may

assume that $1 \in J$ and so there exists $f \in I$ such that $\tilde{h}(f) = 1$ and we have a relation of the form

$$\sum_{i=0}^{r} a_i \alpha^i = 0, \text{ with } a_i \in R \text{ and } h(a_i) = \begin{cases} 1 & \text{if } i = 0 \\ 0 & \text{if } i > 0. \end{cases} \tag{1}$$

We choose r as small as possible.

We may repeat the above argument, replacing α by α^{-1}. Either we obtain an extension $\bar{h} : R[\alpha^{-1}] \longrightarrow C$ or a relation of the form

$$\sum_{i=0}^{s} b_i \alpha^{-i} = 0, \text{ with } b_i \in R \text{ and } h(b_i) = \begin{cases} 1 & \text{if } i = 0 \\ 0 & \text{if } i > 0. \end{cases} \tag{2}$$

Without loss of generality, let us suppose that $r \geq s$. We have $h(b_0) = 1 = h(1)$, hence $b_0 - 1 \in \ker h \subset M$, the unique maximal ideal of the local ring R. If $b_0 \in M$, then $1 \in M$, which is impossible, so $b_0 \notin M$, which implies that b_0 is invertible. Multiplying equation (2) by $b_0^{-1}\alpha^s$, we obtain

$$b_0^{-1} b_s + \cdots + b_0^{-1} b_1 \alpha^{s-1} + \alpha^s = 0. \tag{3}$$

We now multiply this equation by $a_r \alpha^{r-s}$ and we have

$$b_0^{-1} b_s a_r \alpha^{r-s} + \cdots + b_0^{-1} b_1 a_r \alpha^{r-1} + a_r \alpha^r = 0. \tag{4}$$

We notice that (4) is not a copy of (1). If this were the case, then we would have $r = s$ and $a_0 = b_0^{-1} b_s a_r$, which is impossible, because $h(a_0) = 1$ and $h(b_0^{-1} b_s a_r) = 0$. Subtracting equation (4) from equation (1) we obtain an expression contradicting the minimality of r. It follows that we can extend h to $R[\alpha]$ or to $R[\alpha^{-1}]$. □

With this preliminary result we can establish theorem concerning extensions of homomorphisms of subrings of fields.

Theorem 1 *Let R be a subring of a field F, C an algebraically closed field and h a homomorphism from R into C. Then h has a maximal extension $\bar{h} : V \longrightarrow C$ among extensions to rings contained in F. In addition, for every such maximal extension, V is a valuation ring of F.*

PROOF Let $\mathcal{S}$ be the set of all pairs (R_i, h_i), where R_i is a subring of F containing R and $h_i : R_i \longrightarrow C$ a ring homomorphism extension of h. We order $\mathcal{S}$ by the condition $(R_i, h_i) \leq (R_j, h_j)$ if and only if R_i is a subring of R_j and h_i the restriction of h_j to R_i. From Zorn's lemma there exists a maximal element $(V, \bar{h})$, so h has a maximal extension.

If $\alpha \in F^*$, by Lemma 1, $\bar{h}$ has an extension to $V[\alpha]$ or to $V[\alpha^{-1}]$. Since $\bar{h}$ is maximal, either $V = V[\alpha]$ or $V = V[\alpha^{-1}]$. Hence $\alpha \in V$ or $\alpha^{-1} \in V$ and it follows that V is a valuation ring. □

The theorem which we have just proved has an interesting corollary.

Corollary 3 *Let R be a subring of the field F. Then the integral closure $\bar{R}$ of R in F is the intersection of all valuation rings V of F containing R.*

PROOF If $a \in \bar{R}$, then a is integral over R, hence over any valuation ring containing R. From Proposition 1 we know that V is integrally closed, hence $a \in V$. It follows that $\bar{R}$ is contained in the intersection of the valuation rings containing R.

Conversely, suppose that $a \notin \bar{R}$. Then $a \notin R' = R[a^{-1}]$. The reason for this is as follows: If $a \in R'$, then we may write

$$a = c_0 + c_1 a^{-1} + \cdots + c_n a^{-n},$$

with the $c_i \in R$. This implies that

$$a^{n+1} = c_0 a^n + c_1 a^{n-1} + \cdots + c_n,$$

and so $a \in \bar{R}$, a contradiction. Thus $a \notin R' = R[a^{-1}]$, as claimed. This implies that a^{-1} is not a unit in R': If $a^{-1}b = 1$, with $b \in R'$, then $a = a \cdot 1 = aa^{-1}b = b \in R'$, a contradiction. It follows that a^{-1} belongs to a maximal ideal M' of R'.

Let C be an algebraic closure of the field $K = R'/M'$ and h the composition of the standard mapping of R' onto K and the inclusion of K in C. From Theorem 1, $\bar{h}$ has a maximal extension $\bar{h} : V \longrightarrow C$, where V is a valuation ring containing R', and thus R. Now $\bar{h}(a^{-1}) = h(a^{-1}) = 0$, since $a^{-1} \in M'$. Consequently, $a \notin V$, for if $a \in V$, then

$$1 = \bar{h}(1) = \bar{h}(aa^{-1}) = \bar{h}(a)\bar{h}(a^{-1}) = 0,$$

a contradiction. It follows that there is a valuation ring V containing R such that $a \notin V$. This ends the proof. □

Dominance

Let F be a field and R, S local subrings of F, with respective maximal ideals M, N. We say that S dominates R if $R \subset S$ and $M = R \cap N$. (F is not necessarily the fraction field of R or S.) Dominance defines a partial order on the local rings contained in F, which as usual we will note $\leq$. The following elementary result is useful.

Lemma 2 *The following statements are equivalent:*

- **a.** *S dominates R;*
- **b.** *S contains R and N contains M.*
- **c.** *S contains R and every noninvertible element in R is noninvertible in S.*

PROOF The proof is immediate. □

Theorem 2 *If V is a valuation ring of the field F, then V is maximal for the order on local rings. Conversely, if A is maximal for this order, then A is a valuation ring.*

PROOF Let V be a valuation ring and S a local ring dominating V. We note M (resp. N) the maximal ideal of V (resp. S). Suppose that there exists $x \in S \setminus V$. As $x \notin V$, we must have $x^{-1} \in V$. But then $x, x^{-1} \in S$, which implies that $x^{-1} \in S \setminus N$. However, $M = N \cap V$, so $x^{-1} \in V \setminus M$, which implies that $x \in V$, because x is the inverse of x^{-1}. We have a contradiction. Hence V is maximal.

We now consider the converse. Let A be maximal for the order on local rings contained in F, with maximal ideal M_A. We set $K = A/M_A$, where M_A is the maximal ideal of A, and let C be an algebraic closure of K. We let $h : A \longrightarrow C$ be the composition of the standard mapping of A onto K and the injection of K into C. Then h is a ring homomorphism, and by Theorem 1 has a maximal extension $\bar{h} : V \longrightarrow C$, where V is a valuation ring. The kernel of h is M_A. If M_V is the maximal ideal of V, then the kernel of $\bar{h}$ is contained in M_V, so $M_A \subset M_V$. From Lemma 2, V dominates A. As A is maximal, $A = V$. □

We now show that a local ring is always dominated by some valuation ring.

Theorem 3 *Let R be local ring of a field F, then there is a valuation ring V of F which dominates R.*

PROOF We will apply Zorn's lemma to the set of local rings in F dominating R. Let $\mathcal{C} = \{S_i\}_{i\in I}$ be a chain of local rings dominating R and $S = \cup_{i\in I} S_i$. Clearly S is a subring of F. S is also a local ring, as we will now show. Suppose that x and y are nonunits in S. We claim that $x+y$ is also a nonunit. There exist $A, B \in \mathcal{C}$ such that $x \in M_A$ and $y \in M_B$. We may suppose that $A \leq B$. By Lemma 2, $x \in M_B$, and so $x+y \in B$. Now suppose that $x+y$ is a unit in S. Then there exists $C \in \mathcal{C}$ such that $(x+y)^{-1} \in C$, where $B \leq C$. However, this is impossible, because $M_B \subset M_C$, by Lemma 2. Hence $x+y$ is a nonunit in $\mathcal{C}$, as claimed.

Now let x be a nonunit in S and $z \in S$. Then zx is a nonunit in S. (If $zx = u$, with u a unit, then $(u^{-1}z)x = 1$, and so x is a unit.)

We have shown that the nonunits in S form an ideal, therefore S is a local ring, with maximal ideal M_S composed of the set of nonunits in S. We claim that S dominates all the elements of the chain $\mathcal{C}$. If A is an element of the chain, then $A \subset S$. By Lemma 2, it is sufficient to show that $M_A \subset M_S$. Suppose that there exists $x \in M_A$ such that $x \notin M_S$. Then there exists B in the chain such that $x^{-1} \in B$. B necessarily dominates A, (otherwise A dominates B and $x^{-1} \in A$), so $M_A \subset M_B$, which implies that $x^{-1} \notin B$, a contradiction. Thus $M_A \subset M_S$.

We have shown that the chain $\mathcal{C}$ has a maximum. By Zorn's lemma, the set of local rings containing R has a maximal element C. If A is a local ring such that $C \leq A$, then $R \subset A$, so A lies in the set of local rings containing R and so is dominated by C. It follows from Theorem 2 that C is a maximal element for all local rings in K and so is a valuation ring. We have found a valuation ring dominating the local ring R. □

Valuations

In this section we obtain a useful equivalent definition of a valuation ring. We begin with the definition of an ordered group. An ordered group G is an abelian group with a total order $\leq$ such that, for $x, y, z \in G$, we have

$$x \leq y \Longrightarrow zx \leq zy.$$

Let F be a field and G an ordered group. A mapping $v : F \longrightarrow G \cup \{+\infty\}$ is a valuation if, for all $x, y \in F$,

- **a.** $v(x) = +\infty \Longleftrightarrow x = 0$;
- **b.** $v(xy) = v(x)v(y)$;
- **c.** $v(x+y) \geq \min(v(x), v(y))$ (triangle inequality).

As a subgroup of an ordered group is an ordered group, we may suppose that v is surjective. If e is the identity element of the group and $v(x) = e$, for all $x \in F^*$, then we say that v is trivial. We usually assume that this is not the case.

Remark From **b.** we deduce that v defines a surjective homomorphism from $(F^*, \cdot)$ onto G. If e is the identity element of G, then $v(1) = e$ and $v(x^{-1}) = v(x)^{-1}$. In addition, $v(-1) = e$ and $v(-x) = v(x)$. The last point probably needs an explanation. Clearly, $v(-1)^2 = e$. If $v(-1) > e$, then $v(-1)^2 > v(-1)$, i.e., $e > v(-1)$, a contradiction. In the same way, $v(-1) \not< e$, hence $v(-1) = e$. Finally, as $v(-x) = v(-1)v(x)$, we have $v(-x) = v(x)$.

If we set

$$V = \{x \in F : v(x) \geq e\},$$

then V is a ring. If $x \notin V$, then $v(x) < e$, which implies that $v(x^{-1}) > e$, because $v(x)v(x^{-1}) = v(1) = e$. Hence V is a valuation ring. If v is trivial, then clearly $V = F$, otherwise this is not the case.

We now show that any valuation ring may be considered as arising from a valuation. Let V be a valuation ring of F and $G = F^*/V^\times = F^\times/V^\times$. We define an order on G by

$$xV^\times \geq yV^\times \Longleftrightarrow xy^{-1} \in V.$$

The order is well-defined: Suppose that $xy^{-1} \in V$ If $x' = xu$ and $y' = yv$, with $u, v \in V^\times$, then

$$x'y'^{-1} = xu(yv)^{-1} = xy^{-1}uv^{-1} \in V,$$

because xy^{-1} and uv^{-1} belong to V. On the other hand, if $xy^{-1} \notin V$ and $x'y'^{-1} \in V$, then $x'u^{-1}(y'v^{-1})^{-1} \in V$, because $x'y'^{-1}$ and $u^{-1}v$ belong to V. However, $x'u^{-1}(y'v^{-1})^{-1} = xy^{-1}$, so we have a contradiction. Hence $xy^{-1} \notin V$ implies that $x'y^{'-1} \notin V$.

We thus obtain a well-defined order on G, which is clearly total. If $zV^\times \in G$, then

$$zx(zy)^{-1} = xy^{-1} \Longrightarrow zV^\times xV^\times \geq zV^\times yV^\times,$$

so G is an ordered group. Let $v : F^* \longrightarrow G$ be the standard surjective homomorphism and $x, y \in F^*$. Then clearly $v(xy) = v(x)v(y)$. Suppose that $\min(v(x), v(y)) = v(x)$. Then $v(y) \geq v(x)$, which implies that $yx^{-1} \in V$. Now, $(x + y)x^{-1} = 1 + yx^{-1} \in V$, so $v(x + y) \geq v(x) = \min(v(x), v(y))$. An analogous argument applies if $\min(v(x), v(y)) = v(y)$, hence we have $v(x + y) \geq \min(v(x), v(y))$. If we set $v(0) = +\infty$, then v is a valuation on F, whose valuation ring is

$$\tilde{V} = \{x \in F : v(x) \geq V^\times\} = \{0\} \cup \{x \in F^\times : v(x) \geq eV^\times\} = V.$$

Therefore we have shown that a valuation ring may always be considered as the valuation ring of a valuation.

Remark It is natural to ask whether every field F contains a valuation ring which is not equal to F itself. If F is an algebraic extension of a finite field, then it can be shown that, for any element $x \in F^*$, there is a strictly positive integer n such that $x^n = 1$. If v is a valuation on F, then $v(x)^n = v(x^n) = e$, where e is the identity of the ordered group associated to v. If $v(x) > e$, then $v(x)^2 > v(x)e = v(x)$. Continuing in the same way, we obtain a strictly increasing sequence and so $v(x)^n \neq e$. In the same way we obtain a decreasing sequence if $v(x) < e$. It follows that $v(x) = e$. Thus v is trivial and so the only valuation ring contained in F is F itself.

In the next section we will consider those valuation rings where the range of the valuation is $\mathbf{Z} \cup \{+\infty\}$. This class of valuation rings is the most important.

Discrete valuation rings

Let F be a field. A *discrete valuation* on F is a surjective mapping $v : F \longrightarrow \mathbf{Z} \cup \{+\infty\}$ such that, for $x, y \in F$,

- **a.** $v(x) = +\infty \Longleftrightarrow x = 0$;
- **b.** $v(xy) = v(x) + v(y)$;

- **c.** $v(x+y) \geq \min(v(x), v(y))$ (triangle inequality).

Notation If F is a field, then we note $\mathcal{V}(F)$ the set of discrete valuations defined on F.

Remark From **b.** we deduce that v defines a surjective homomorphism from $(F^*, \cdot)$ onto $(\mathbf{Z}, +)$. Thus $v(1) = 0$ and $v(x^{-1}) = -v(x)$. In addition, $v(-1) = 0$ and $v(-a) = v(a)$.

Examples

- Consider the field of rational numbers $\mathbf{Q}$ and fix a prime number p. For $x = \frac{p^r m}{n} \in \mathbf{Q}^*$, with $r \in \mathbf{Z}$, $p \nmid m$ and $p \nmid n$, we set $v_p(x) = r$. If, in addition, we set $v_p(0) = +\infty$, then v_p is a discrete valuation on $\mathbf{Q}$. (This valuation is called the p-adic valuation on $\mathbf{Q}$.) We may find an expression for the nth power of the prime ideal $\mathbf{Z}p$ of $\mathbf{Z}$ in terms of the p-adic valuation v_p, namely $(\mathbf{Z}p)^n = \{x \in \mathbf{Z} : v_p(x) \geq n\}$.

- Let K be a field and $F = K(X)$. For $\frac{f}{g}$, we define $v(\frac{f}{g}) = \deg g - \deg f$ and we set $v(0) = +\infty$. Then v is a discrete valuation on F.

- For a field K, consider the field of rational functions $K(X)$. We fix an irreducible polynomial $P \in K[X]$. Any nonzero element of $K(X)$ can be written in a unique way $\frac{P^n G}{H}$, where $n \in \mathbf{Z}$ and G, H are polynomials in $K[X]$ not divisibles by P. Then $v(\frac{P^n G}{H}) = n$, together with $v(0) = \infty$, defines a discrete valuation on $K(X)$.

If $v(x) \neq v(y)$, then we may strengthen the triangle inequality.

Proposition 4 *If $x, y \in F$ and $v(x) \neq v(y)$, then $v(x+y) = \min(v(x), v(y))$ (strict triangle inequality).*

PROOF We may suppose that $v(x) < v(y)$. Then

$$v(x) = v(x + y + (-y)) \geq \min(v(x+y), v(-y)) = \min(v(x+y), v(y)).$$

If $v(y) = \min(v(x+y), v(y))$, then $v(x) \geq v(y)$, a contradiction, so $\min(v(x+y), v(y)) = v(x+y)$ and we have $v(x) \geq v(x+y)$, i.e., $\min(v(x), v(y)) \geq v(x+y)$. It follows that $v(x+y) = \min(v(x), v(y))$. □

Corollary 4 *If v is a discrete valuation on the field F, $n \geq 2$ and $x_1, \ldots x_n$ nonzero elements of F satisfying the equality $x_1 + \cdots + x_n = 0$, then the set $S = \{v(x_1), \ldots, v(x_n)\}$ has no strict minimum. In particular, there exist $1 \leq i < j \leq n$ such that $v(x_i) = v(x_j)$.*

PROOF Suppose that the set S has a strict minimum. We may suppose that this is $v(x_1)$. Then

$$v(x_2 + \cdots + x_n) \geq \min(v(x_2), \ldots, v(x_n)) > v(x_1).$$

From the strict triangle inequality $v(x_1 + \cdots + x_n) = v(x_1)$. However, $v(x_1 + \cdots + x_n) = +\infty$ and $v(x_1) \neq +\infty$, because $x_1 \neq 0$. Thus we have a contradiction and so the set S has no strict minimum. □

We now establish a relation between discrete valuations and valuation rings.

Proposition 5 *If v is a discrete valuation on a field F, then $V = \{x \in F : v(x) \geq 0\}$ is a valuation ring, with maximal ideal $M = \{x \in F : v(x) \geq 1\}$. The group of units in V is the set $U = \{x \in V : v(x) = 0\}$.*

PROOF As $0 \in V$, V is nonempty. Using **c.** we deduce that the sum of two elements in V is also in V; as $v(-x) = v(x)$, the additive inverse of an element in V is also in V. Thus V is an additive subgroup of $(F, +)$. Also, from **b.** we deduce that the product of two elements in V is also in V. Finally, $1 \in V$, because $v(1) = 0$. It follows that V is a subring of F.

If $x \notin V$, then $v(x) < 0$, so $v(x^{-1}) = -v(x) > 0$, proving that $x^{-1} \in V$. Thus V is a valuation ring.

The element x is a unit in V if and only if x and x^{-1} both belong to V, which is the case if and only if $v(x) = 0$. Thus the group of units U is composed of the elements $x \in V$ such that $v(x) = 0$. The nonunits are those elements $x \in V$ such that $v(x) \neq 0$, i.e., those elements x with $v(x) \geq 1$, which is precisely the unique maximal ideal M. □

Definition A valuation ring V arising from a discrete valuation on a field F is called a *discrete valuation ring*, which is often noted DVR.

Proposition 6 *A DVR is euclidean.*

PROOF Let v be a discrete valuation defined on the field F and V the associated valuation ring. We define $N : V \longrightarrow \mathbf{Z}_+$ by $N(0) = 0$ and $N(x) = v(x)$, for $x \in V^*$. Suppose that $x, y \in V$, with $y \neq 0$. We have to find $q, r \in V$ such that

$$x = qy + r,$$

with $r = 0$ or $N(r) < N(y)$. On the one hand, if $v(x) \geq v(y)$, then $v(\frac{x}{y}) = v(x) - v(y) \geq 0$, so $\frac{x}{y} \in V$ and we can set $q = \frac{x}{y}$, $r = 0$. On the other hand, if $v(x) < v(y)$, then we can set $q = 0$, $r = x$ and we have $N(x) < N(y)$. □

An element t in a DVR such that $v(t) = 1$ is called a *uniformizer*. As the discrete valuation v is surjective, such an element always exists. As a uniformizer is not a unit, a DVR cannot be a field.

Proposition 7 *If t is a uniformizer in a DVR V, then t is a generator of the unique maximal ideal M, i.e., $M = (t)$. Conversely, if t' is a generator of M, then t' is a uniformizer.*

PROOF Since $v(t) = 1$, Proposition 7 ensures that $(t) \subset M$. If $x \in M$, then $v(x) \geq 1$, hence

$$v(xt^{-1}) = v(x) - v(t) \geq 1 - 1 = 0,$$

so $xt^{-1} \in V$ and thus $x = xt^{-1}t \in (t)$. Therefore $M \subset (t)$.

Now suppose that $M = (t')$. Then $t = ct'$, for some $c \in V$. Hence

$$1 = v(t) = v(c) + v(t').$$

Since $v(t') \geq 1$ and $v(c) \geq 0$, we must have $v(t') = 1$. □

Corollary 5 *If v and v' are distinct discrete valuations on the field F, with respective discrete valuation rings V and V', then $V \neq V'$. If M and M' are the corresponding maximal ideals, then $M \neq M'$.*

PROOF Let t be a generator of the maximal ideal M of V. As $v \neq v'$, there exists $x \in F$ such that $v(x) \neq v'(x)$. Let $v(x) = n$ and $v'(x) = m$. We may suppose that $n < m$. Then $v(xt^{-m}) = n - m < 0$ and $v'(xt^{-m}) = m - m = 0$. Hence $xt^{-m} \notin V$ and $xt^{-m} \in V'$. Therefore $V \neq V'$.

As for the maximal ideals, we have $v(xt^{-m+1}) = n-m+1 \leq 0$ and $v'(xt^{-m+1}) = m-m+1 = 1$, so $xt^{-m+1} \notin M$, but $xt^{-m+1} \in M'$. Hence $M \neq M'$. □

Remark From Corollary 5 we deduce that the mapping ϕ sending a discrete valuation to its valuation ring is a bijection from the discrete valuations on F onto the discrete valuation rings contained in F. Also, the mapping ψ sending a discrete valuation to the maximal ideal of its valuation ring is a bijection from the discrete valuations on F onto the maximal ideals of the the discrete valuation rings contained in F.

Proposition 8 *A DVR is infinite as is its group of units.*

PROOF Let V be a DVR contained in a field F and v the valuation on F defining V, i.e., $V = \{x \in F : v(x) \geq 0\}$. If t is a uniformizer of R, then $v(t^n) = n > 0$, for $n \in \mathbf{N}^*$, and so $t^n \in V$. As the t^n are distinct, V is infinite.

Let us now consider elements of the form $1 + t^n$. As $v(1) = 0$ and $v(t^n) = n$, from the strict triangle inequality (Proposition 4), we have $v(1 + t^n) = 0$ and so $1 + t^n$ is a unit. Since the elements $1 + t^n$ are distinct, there is an infinite number of units in V. □

The next result is fundamental.

Proposition 9 *If t is a uniformizer in a DVR V, then every nonzero element $x \in F$, the field of fractions of V, can be expressed uniquely in the form $x = ut^n$, where u is a unit in V and $n \in \mathbf{Z}$.*

PROOF Let $n = v(x)$. This implies that xt^{-n} is a unit u in V. Then $x = ut^n$. To prove the uniqueness, notice that

$$x = ut^n \Longrightarrow v(x) = v(u) + nv(t) = 0 + n = n,$$

so n is determined by x. Then $u = xt^{-n}$ and we have the desired uniqueness. □

Corollary 6 *If $V \subset W$ are DVRs with the same field of fractions F, then $V = W$.*

PROOF Let M be the maximal ideal of V, v the discrete valuation on F whose valuation ring is V and t a uniformizer in V. Take $x \in W$ and suppose that $v(x) = n$. If $n \geq 0$, then $x \in V$. If $n < 0$, then $v(xt^{-n}) = 0$, which implies that $u = xt^{-n}$ is a unit in V. Now, $t^{-1} = u^{-1}xt^{-1-n} \in W$, since $u^{-1} \in V \subset W$, $x \in W$ and $-1-n \geq 0$. It follows that all powers of t (negative or positive) belong to W. However, every element of F^* can be written as a power of t multiplied by a unit in V. As all the units of V lie in W, we see that $F^* \subset W$ and so we have $F \subset W$, a contradiction. Therefore $V = W$. □

We have seen already in Proposition 3 that a noetherian valuation ring is a PID and that any ideal I is a power of the unique maximal ideal M. For a DVR we have a proof of this, but without the noetherian condition.

Proposition 10 *If V is a DVR, with maximal ideal M, and I a proper ideal of V, then $I = M^s$, for some $s \in \mathbf{N}^*$. Also, there is a unique nonzero prime ideal in a DVR.*

PROOF Choose $x \in I$ such that $n = v(x)$ is as small as possible. From Proposition 9 we may write $x = ut^n$, where t is a uniformizer and u a unit of V. Then $t^n = u^{-1}x \in I$. From Proposition 10, $M = (t)$ and so $M^n = (t^n) \subset I$.

Conversely, let $y \in I$; from the minimality of n, $v(y) = k \geq n$. By Proposition 9, we may write $y = u't^k$, where u' is a unit in V. Since $k \geq n$, we have $y \in (t^n) = M^n$, so $I \subset M^n$ and it follows that $I = M^n$.

Finally, if $P = (t^n)$ is a prime ideal, then we must have $n = 1$, so $P = M$, i.e., there is only one prime ideal in R, namely M. □

Remarks a. If $x \in V$, then $v(x)$ is the largest nonnegative integer k such that $v(x) \in M^k$.
b. For a nonnegative integer k, we have an expression for M^k in terms of the valuation, namely $M^k = \{x \in V : v(x) \geq k\}$.

Corollary 7 *A uniformizer in a DVR is prime.*

PROOF From Proposition 10 we see that a DVR V is a PID, hence a UFD. This implies that a generator of the maximal ideal M of V is irreducible, hence prime. □

We have shown that if V is a DVR, then there exists a non-unit $t \in V$ (in fact, a prime element) such that any $x \in V^*$ may be written uniquely $x = ut^n$, where $n \in \mathbf{N}$ and u is a unit in V. This result has a converse.

Proposition 11 *If V is an integral domain and $t \in V$ is a nonunit such that, for all $x \in V^*$ we may write uniquely $x = ut^n$, where $n \in \mathbf{N}$ and u is a unit in V, then V is a DVR.*

PROOF If F is the field of fractions of V, then an element $x \in F^*$ may be written uniquely $x = ut^n$, where $n \in \mathbf{Z}$ and u is a unit in V. Setting $v(x) = n$, for $x \in F^*$, and $v(0) = \infty$, we obtain a valuation on F: Clearly, v is a surjective mapping of F onto $\mathbf{Z}$ and $v(xy) = v(x) + v(y)$. It remains to show that $v(x + y) \geq \min(v(x), v(y))$.

If $x = 0$, $y = 0$ or $y = -x$, then the inequality is clearly satisfied, so suppose that we do not have one of these cases. Then we may write $x = ut^m$, $y = u't^n$ and $v(x) = m$, $v(y) = n$. Without loss of generality, let us assume that $m \leq n$. Then

$$v(x + y) = v(ut^m + u't^n) = v((t^m(u + u't^{n-m})) = v(t^m) + v(u + u't^{n-m}) = m + v(u + u't^{n-m}).$$

As $u + u't^{n-m} \in V$, we have $v(u + u't^{n-m}) \geq 0$, so $v(x + y) \geq m = \min(v(x), v(y))$.

To conclude, clearly $V = \{x \in F : v(x) \geq 0\}$, so V is a DVR. □

Remarks a. It is natural to ask why we have chosen t a nonunit. If t were a unit, then we could not express every $x \in V$ uniquely in the form $x = ut^n$, for in this case we would also have, for example, $x = (ut)t^{n-1}$, with ut a unit.
b. As $v(t) = 1$, t is a uniformizer, so, from Corollary 10, t must be a prime.

We have shown that a DVR is necessarily a PID. Of course, there are PIDs which are are not DVRs, e.g., the ring of integers $\mathbf{Z}$. However, we may characterize the PIDs which are DVRs.

Proposition 12 *A PID is a DVR if and only if it has a unique nontrivial maximal ideal.*

PROOF Let R be a PID. If R is a DVR, then R is a valuation ring and so has a unique maximal ideal, which is nontrivial because it contains a nonzero element, namely a uniformizer.

Now suppose that R has a unique nontrivial maximal ideal. By hypothesis, M is principal, i.e., $M = (a)$, for some $a \in R^*$, which is necessarily irreducible. (In fact, if a' is another irreducible element, then $a' = va$, where v is a unit, since we must have $(a') = (a)$.) We claim

that $\cap_{n=1}^{\infty} M^n = \{0\}$. Suppose that $x \in M^n$, for $n \geq 1$. Then $a^n | x$, for $n \geq 1$. Given that R is a UFD, this can only be possible if $x = 0$.

Now let $x \in R^*$. Since $\cap_{n=1}^{\infty} M^n = \{0\}$, there exists n such that $x \in (a^n)$ and $x \notin (a^{n+1})$. Thus $x = ua^n$, with $u \notin M$, i.e., u a unit. The expression $x = ua^n$ is a factorization into prime elements. As R is a UFD, the power n is unique.

We have shown that $x = ua^n$, with n and u unique. We set $v(x) = n$. If $\beta = \frac{x}{y} \in F^*$, where F is the fraction field of R, and $x = ua^m$, $y = u'a^{m'}$, then $\beta = u_0 a^k$, where u_0 is a unit and $k \in \mathbf{Z}$. This expression is unique: If $u_0 a^k = u_0' a^{k'}$, with $k' \geq k$, then $u_0 = u_0' a^{k'-k} \in R^*$. By uniqueness, $k' - k = 0$ and so $u_0 = u_0'$. This shows that the expression for β is unique. For $\beta \in F^*$, we set $v(\beta) = k$, where $\beta = u_0 a^k$, with u_0 a unit and $k \in \mathbf{Z}$. We also set $v(0) = +\infty$. Then v is a discrete valuation such that $R = \{x : v(x) \geq 0\}$. □

Remark From the above result we obtain an alternative definition of a DVR: V is a DVR in F if the fraction field of V is F and V is a PID with a unique nontrivial maximal ideal. From Proposition 3, we deduce that if V is a noetherian valuation ring in a field F, then V is a DVR.

Dedekind domains

We recall the definition of a Dedekind domain: a *Dedekind domain* is a noetherian domain, integrally closed in its fraction field and such that all nonzero prime ideals are maximal.

It is known that the localization D_P of a Dedekind domain at a nonzero prime ideal P is a Dedekind domain, which is also a PID. From the remark after Proposition 12, this implies that D_P is a DVR. This has a converse. However, we need a preliminary result, but first a definition.

Definition Let R be an integral domain, with fraction field F and $I \subset F$ a fractional ideal of R. For a prime ideal P of R we write I_P for the fractional ideal of R_P defined by $I_P = R_P I$. (In particular, P may be a maximal ideal M.)

Lemma 3 *If R is an integral domain, with field of fractions F, and I a fractional ideal of R, then $I = \cap_M I_M$, where the intersection is taken over all maximal ideals of R.*

PROOF Let $x \in \cap_M I_M$. As $\cap_M I_M \subset F$, there exist $a, b \in R$, with $b \in R^*$, such that $x = \frac{a}{b}$. We set $J = \{y \in R : ya \in bI\}$. Notice that J is well-defined: If $\frac{a}{b} = \frac{c}{d}$ and $yc \in dI$, then

$$ya = y\frac{bc}{d} = \frac{b}{d}du = bu,$$

where $u \in I$. Thus $ya \in bI$. In the same way, $ya \in bI$ implies that $yc \in dI$. Hence J is well-defined. As $0 \in J$, J is not empty. A simple verification shows that J is an ideal in R.

Let M be a maximal ideal in R; then $x = \frac{a}{b}$ is an element of I_M, because $x \in \cap_M I_M$. As $x \in I_M$, $x = \frac{c}{d}$, where $c \in I$ and $d \notin M$. By definition, we have $d \in J \setminus M$ and so J is not contained in M. It follows that J is contained in no maximal ideal and so $J = R$. In particular, $1 \cdot a \in bI$, which implies $x = \frac{a}{b} \in I$. We have shown that $\cap_M I_M \subset I$. It is clear that $I \subset \cap_M I_M$, so we have the required equality. □

Corollary 8 *If $I \subset J$ are (integral) ideals in a commutative ring R such that $I_M = J_M$ for all maximal ideals M containing I, then $I = J$.*

PROOF Adapting Lemma 3 we obtain

$$I = \cap_M I_M \qquad \text{and} \qquad J = \cap_M J_M,$$

where the intersection is taken over all maximal ideals M of R. However, we may restrict the intersection to maximal ideals containing I. Indeed, if M is a maximal ideal not containing I, then $I \cap (R \setminus M)$ is nonempty. If $x \in I \cap (R \setminus M)$, then $\frac{1}{x} \in R_M$, so $\frac{x}{1}$ is a unit in R_M. However, $\frac{x}{1} \in I_M$, so the ideal I_M contains a unit of R_M, which implies that $I_M = R_M$. Since $I \subset J$, we have $J \cap (R \setminus M)$ is nonempty, so $J_M = R_M$. Thus, for all maximal ideals M not containing I, we have $I_M = J_M$. Hence, for all maximal ideals M, $I_M = J_M$ and it follows that $I = J$. □

We may now prove the converse referred to above.

Theorem 4 *Let R be a noetherian integral domain. If, for all nonzero maximal ideals M, the local ring R_M is a DVR, then R is a Dedekind domain.*

PROOF We need to show that a nonzero prime ideal in R is maximal and that R is integrally closed in its field of fractions F.

Let P be a nonzero prime ideal in R and M a maximal ideal containing P. By hypothesis R_M is a DVR, so $R_M P = R_M M$, because a DVR has a unique prime ideal (Proposition 10). This implies that $P = M$, and so P is maximal.

Now let $x \in F$ be integral over R. Then x is integral over R_M, for every nonzero maximal ideal M and so belongs to R_M, from Proposition 1. Using Lemma 3 with $I = R$, we obtain $x \in R$, and so R is integrally closed in F. □

Discrete valuations and Dedekind domains

On the fraction field of a Dedekind domain we may define a particular collection of discrete valuations. If P is a nonzero prime ideal in D, a Dedekind domain, then we have already seen that the localization D_P is a DVR, hence the field of fractions F of D_P has a discrete valuation, which we note v_P. Thus, for any $x \in D_P$, $v_P(x)$ is the largest integer $k \geq 0$ such that $x \in \bar{P}^k$, where $\bar{P} = D_P P$, the unique maximal ideal in D_P. In addition, for $k \geq 0$, $\bar{P}^k = \{x \in D_P : v_P(x) \geq k\}$. The following theorem shows that, for $x \in D$, $v_P(x)$ is the largest integer $k \geq 0$ such that $x \in P^k$; also $P^k = \{x \in D : v_P(x) \geq k\}$.

Theorem 5 *Let D be a Dedekind domain with fraction field F. Then every nonzero prime ideal P determines a discrete valuation v_P on F, which is the unique valuation on F satisfying the conditions:*

- **a.** *$v_P(x) = 0$, for all $x \in D \setminus P$;*
- **b.** *$v_P(x) = k$, for all $x \in P^k \setminus P^{k+1}$.*

PROOF If $x \in D \setminus P$, then x is a unit in D_P, because $x \notin \bar{P}$, hence $v_P(x) = 0$.

We now consider the case where $x \in P$. Suppose that $x \in P^k \setminus P^{k+1}$. We claim that $x \in \bar{P}^k \setminus \bar{P}^{k+1}$. Clearly, $x \in \bar{P}^k$. We must show that $x \notin \bar{P}^{k+1}$. This results from the fact that $\bar{P}^{k+1} \cap D = P^{k+1}$, which we will now prove. It is evident that $P^{k+1} \subset \bar{P}^{k+1} \cap D$, so we only need to establish the reverse inclusion. Let $\frac{y}{u} \in \bar{P}^{k+1} \cap D$, with $y \in P^{k+1}$ and $u \notin P$; then $\frac{y}{u} = d \in D$. Thus $y = ud \in D$ and so $ud \in P^{k+1}$ and it follows that $(u)(d) \subset P^{k+1}$. As $u \notin P$, $P \nmid (u)$ and so $P^{k+1} | (d)$, which implies that $d \in P^{k+1}$. So we have the reverse inclusion.

Let t be a uniformizer of v_P; then $\bar{P}^k \setminus \bar{P}^{k+1} = (t^k) \setminus (t^{k+1})$. Thus $x = at^k$ and $t \nmid a$, which implies that a does not belong to $\bar{P}$ and so is a unit. It follows that $v_P(x) = k$.

Suppose now that v' is a discrete valuation satisfying the conditions **a.** and **b.** Then $v'(x) = 0 = v_P(x)$, for all $x \in D \setminus P$. If $x \in P^k \setminus P^{k+1}$, then $v'(x) = k = v_P(x)$. Therefore, for every

$x \in D$, $v'(x) = v_P(x)$. Every nonzero element of the field of fractions F of D is of the form xy^{-1}, where $x, y \in D^*$, and

$$v'(xy^{-1}) = v'(x) - v'(y) = v_P(x) - v_P(y) = v_P(xy^{-1}).$$

It follows that $v'(z) = v_P(z)$, for all $z \in F$. □

Definition The discrete valuations which we defined in Theorem 5 are called P-adic valuations on D. These discrete valuations generalize the p-adic valuations previously defined on $\mathbf{Q}$.

Remark If P is a nontrivial prime ideal of a Dedekind domain D, then the localization D_P is also a Dedekind domain with unique nonzero prime ideal $D_P P$. Then the field of fractions F of D_P has a D_P-adic valuation. As the P-adic and D_P-adic valuations coincide on D, they must be equal.

We may determine the P-adic valuations of an element in $D \setminus \{0\}$ using the decomposition of an ideal into prime ideals.

Proposition 13 *Let $x \in D \setminus \{0\}$ and*

$$(x) = P_1^{e_1} \cdots P_s^{e_s}$$

and P be a prime ideal in D. Then $v_P(x) = 0$, if P is not one of the ideals $P_1, \ldots, P_s$. On the other hand, if $P = P_i$, then $v_P(x) = e_i$.

PROOF Fix a prime ideal P. If $P \neq P_i$, for some P_i, then $x \in D \setminus P$. (If $x \in P$, then $(x) \subset P \Longrightarrow P|(x) \Longrightarrow P = P_i$, for some i, a contradiction.) Thus $v_P(x) = 0$. If $P = P_i$, then $P^{e_i}|(x)$ and $P^{e_i+1} \nmid (x)$, so $x \in P^{e_i} \setminus P^{e_i+1}$ and it follows that $v_P(x) = e_i$. □

Theorem 5 has a useful corollary.

Corollary 9 *Let D be a Dedekind domain, with field of fractions F, and suppose that $x, y \in D^*$. Then $x|y$ if and only if $v_P(x) \leq v_P(y)$, for any P-adic valuation v_P.*

PROOF If $x|y$ in D, then there exists $w \in D$ such that $y = wx$ and so $v_P(y) = v_P(w) + v_P(x) \geq v_P(x)$.

Conversely, if $v_P(y) \geq v_P(x)$, for all prime ideals P of D, then $v_P(yx^{-1}) \geq 0$, for all prime ideals P of D, i.e., $yx^{-1} \in \cap D_P$. From Lemma 3, this intersection is equal to D, which implies that $x|y$. □

The following result is also interesting.

Proposition 14 *Let D be a Dedekind domain, with field of fractions F. For $x \in D^*$, there are only a finite number of prime ideals P such that $v_P(x) \neq 0$.*

PROOF If $x \in D^*$, then $v_P(x) \neq 0$ if and only if $(x) \subset P$, i.e., $P|(x)$. However, from the unique factorization of ideals, we know that there can only be a finite number of prime ideals dividing (x), hence the result. □

Remark Distinct prime ideals give rise to distinct discrete valuations. If $P_1 \neq P_2$, then $P_1 \not\subset P_2$, because the ideals P_1 and P_2 are maximal. Hence there exists x in P_1 which is not in P_2. Then

$v_{P_1}(x) \geq 1$ and $v_{P_2}(x) = 0$, so $v_{P_1} \neq v_{P_2}$.

From Theorem 5 we know that for any P valuation v_P, we have $v_P(D) \geq 0$. We now may ask whether all discrete valuations v on the field of fractions of a Dedekind domain D, such that $v(D) \geq 0$, are P valuations, for some prime ideal P. This is in fact the case.

Proposition 15 *Let D be a Dedekind domain, which is not a field, with field of fractions F. Suppose that v is a discrete valuation on F such that $v(D) \geq 0$. Then there is a nonzero prime ideal P in D such that $v = v_P$.*

PROOF Let V be the valuation ring defined by the discrete valuation v. As $V = \{x \in F : v(x) \geq 0\}$, D is a subset of V. Let $M_v = \{x \in F : v(x) \geq 1\}$ be the maximal ideal of V and $M = M_v \cap D$. As M_v is a prime ideal in V, M is a prime ideal in D. This prime ideal is nontrivial: As D is not a field, D has nonzero elements, which are not invertible; however, these elements belong to M_v, so $M \neq \{0\}$. Thus M is a nonzero prime ideal in D.

Now, D_M is a DVR, as is V, and D_M is included in V: if $x \in D_M^*$, then $x = \frac{a}{b}$, with $a \in D^*$ and $b \in D \setminus M \subset D \setminus M_v$. This implies that $v(x) = v(a) - v(b) = v(a) \geq 0$, hence $D_M \subset V$. From Corollary 5, we have $D_M = V$ and it follows that $v = v_M$. □

Remark From the remark after Proposition 14 and Proposition 15, there is a bijection from the set of nonzero maximal ideals in D onto the set of valuations on F such that $v(D) \geq 0$.

From Proposition 15 we may deduce an interesting result concerning the DVRs containing a given Dedekind domain.

Corollary 10 *If D is a Dedekind domain, then the DVRs in the field of fractions F of D which contain D and have F for field of fractions are the localizations of D with respect to a nonzero prime ideal in D.*

PROOF Clearly $D \subset D_P$, for any prime ideal P in D. Now suppose that V is a DVR containg D. There exists a discrete valuation v on F, the field of fractions of D, whose valuation ring is V. As $v(V) \geq 0$ and $D \subset V$, we have $v(D) \geq 0$. From Proposition 15, there exists a nonzero prime ideal P in D such that $v = v_P$. Hence $V = D_P$. □

Remark From Lemma 3 and Corollary 10, we deduce that a Dedekind domain D is the intersection of all the DVRs in the fraction field F of D containing D.

Now we aim to find an expression for the residue field of the valuation v_P. We need a result from the theory of localizations: If M is a maximal ideal in a commutative ring R, then the quotient field R/M is isomorphic to the quotient field $R_M/R_M M$.

Proposition 16 *Let D be a Dedekind domain, with field of fractions F, and P a nontrivial prime ideal in D. Then the residue field of the P-adic valuation v_P is isomorphic to the field D/P.*

PROOF By definition of the P-adic valuation v_P, the valuation ring of v_P is D_P. This has a unique maximal ideal $D_P P$. Thus the residue field of the valuation v_P is $D_P/D_P P$, which is isomorphic to D/P. □

To close this section, we consider valuations on certain extensions of a Dedekind domain. If D is a Dedekind domain, with field of fractions F, and L a finite separable extension of F, then

the integral closure C of D in L is a Dedekind domain. We now fix a prime ideal P in D. There exist distinct prime ideals $Q_1, \ldots, Q_s \in C$ such that $CP = Q_1^{e_1} \cdots Q_s^{e_s}$, with $e_1, \ldots, e_s \in \mathbf{N}^*$. Our aim here is to consider the relation between the Q_i-adic valuations on the field of fractions of C, namely L, and the P-adic valuation on F. We will need the following result from the theory of Dedekind domains.

Proposition 17 *Let D be a Dedekind domain, with field of fractions F, L a finite separable extension of F, and C the integral closure of D in L, then C is a Dedekind domain and every nonzero maximal ideal Q in C lies over a unique nonzero maximal ideal P in D and $P = Q \cap D$.*

Now we have

Theorem 6 *The restriction of the Q_i-adic valuation $v_{Q_i} = v_i$ to F is $e_i v_P$, i.e., $v_{i|_F} = e_i v_P$. In particular, $v_i(F^*) = e_i \mathbf{Z}$.*

PROOF For $x \in D \setminus \{0\}$, Proposition 13 ensures that there exists an ideal J such that $P \nmid J$ and $Dx = P^{v_P(x)} J$. In the light of this observation we have

$$Cx = CDx = C(P^{v_P(x)} J) = (CP)^{v_P(x)}(CJ) = (Q_1^{e_1} \cdots Q_s^{e_s})^{v_P(x)}(CJ)$$

Each Q_i lies over P, but no Q_i contains CJ. (Q_i lies over a unique prime ideal in D, namely P, and $P = Q_i \cap D$; if Q_i contains CJ, then P contains J, a contradiction.) Hence the power of Q_i in Cx is $e_i v_P(x)$ and the result follows from Proposition 13. □

Remark If we set $v_i' = \frac{1}{e_i} v_i$, then the image of v_i' restricted to F^* is $\mathbf{Z}$, so v_i' is a discrete valuation on F.

From Proposition 17 we may deduce another result.

Proposition 18 *Let V be a DVR, with field of fractions F, L a finite separable extension of F, and C the integral closure of V in L; then C is a Dedekind domain. Also, C has a finite number of nonzero prime ideals. In addition, the localization of C with respect to any of its prime ideals dominates V.*

PROOF As V is a DVR, V is a PID, hence a Dedekind domain, and so its closure C in L is a Dedekind domain. Any nonzero prime ideal in C must lie over a nonzero prime ideal in V. As there is only a finite number of nonzero prime ideals in C lying over a given nonzero prime ideal in V and V has a unique nonzero prime ideal, C has a finite number of prime ideals.

Let Q be a prime ideal in C and C_Q the localization of C with respect to Q. As $V \subset C$ and $C \subset C_Q$, we have $V \subset C_Q$. Now let M be the unique maximal ideal of V. The unique maximal ideal of C_Q is $\bar{Q} = C_Q Q$. To show that C_Q dominates V we must establish that $M = \bar{Q} \cap V$, or equivalently that $M \subset \bar{Q}$ (Lemma 2). However, as Q lies over M, $M \subset Q \subset \bar{Q}$ and so C_Q dominates V. □

P-adic valuations on ideals

We may extend P-adic valuations to ideals. We fix a nonzero prime ideal P. Let I be an ideal in the Dedekind domain D. If $I = \{0\}$, then we set $V_P(I) = +\infty$, and if $I \neq \{0\}$, we define

$$V_P(I) = \min\{v_P(x) : x \neq 0, x \in I\}.$$

By definition, $V_P(I) \leq v_P(x)$, for all $x \in I$. From Proposition 14, for a given nonzero ideal I, $V_P(I) \neq 0$, for at most a finite number of prime ideals P. We will write $Prim(D)$ for the set of nonzero prime ideals P in D. (We recall that these are maximal ideals.)

If I is a nonzero ideal in a Dedekind domain D and $P \in Prim(D)$, then there exists a unique nonnegative integer n such that $I = P^n Q$, where $P \nmid Q$. We claim that $n = V_P(I)$. Let us set $m = \min\{v_P(x) : x \neq 0, x \in I\}$. We choose $x \in I$ such that $v_P(x) = m$. Then $(x) = P^{v_P(x)}Q'$, where $P \nmid Q'$. As $I|(x)$, we have $P^n|(x)$, which implies that $m \geq n$. Moreover, if $m > n$, then all the elements $x \in I$ are such that $v_P(x) \geq n+1$, which implies that $P^k|I$, for some $k \geq n+1$, because $P^k = \{x \in D : v_P(x) \geq k\}$. This is a contradiction, so $m = n$. We have established the claim.

Proposition 19 *If D is a Dedekind domain and I an ideal in D, then*

$$I = \{x \in D : v_P(x) \geq V_P(I), \forall P \in Prim(D)\}.$$

PROOF Let us consider the ideal I_P in D_P. We have $I = P^{V_P(I)}Q$, where $P \nmid Q$, from which we deduce $I_P = \bar{P}^{V_P(I)}$. (As $P \nmid Q$, $\bar{Q} = D_P Q$ contains units, which implies that $\bar{Q} = D_P$.) Now, for $n \geq 0$, $\bar{P}^n = \{x \in D_P : v_P(x) \geq n\}$, hence $I_P = \{x \in D_P : v_P(x) \geq V_P(I)\}$.

Using Lemma 3, we obtain

$$I = (\cap_{P \in Prim(D)} I_P) \cap D = \cap_{P \in Prim(D)} (I_P \cap D) = \cap_{P \in Prim(D)} \{x \in D : v_P(x) \geq V_P(I)\},$$

i.e.,

$$I = \{x \in D : v_P(x) \geq V_P(I), \forall P \in Prim(D)\},$$

as required. □

We may consider sums and products of ideals.

Proposition 20 *If D is a Dedekind domain, P a nonzero prime ideal in D and I, J ideals in D, then*

$$V_P(I+J) \geq \min\{V_P(I), V_P(J)\} \quad \textit{and} \quad V_P(IJ) = V_P(I) + V_P(J).$$

PROOF First we handle the sum. Let $x \in I$, $y \in J$ such that $v_P(x+y) = V_P(I+J)$. Then

$$v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq \min\{V_P(I), V_P(J)\}, \quad \text{i.e.,} \quad v_P(I+J) \geq \min\{V_P(I), V_P(J)\}.$$

We now turn to the product. As above we write $\bar{P}$ for the maximal ideal in D_P, i.e., $\bar{P} = D_P P$. Then

$$I_P = \{x \in D_P : v_P(x) \geq V_P(I)\} = \bar{P}^{V_P(I)}$$

and

$$J_P = \{x \in D_P : v_P(x) \geq V_P(J)\} = \bar{P}^{V_P(J)}.$$

Therefore,

$$(IJ)_P = I_P J_P = \bar{P}^{V_P(I)+V_P(J)} \Longrightarrow V_P(IJ) = V_P(I) + V_P(J),$$

as required. □

Remark The mappings V_P which we have just defined on the ideals of a Dedekind domain have certain properties of valuations, but are not strictly speaking valuations. The reason for this is that the ideals do not form a ring but only a monoid, because in general they do not have an

additive inverse.

Field extensions and DVRs

Let F/K be a finite separable field extension. First we consider the intersection of a DVR in F with K.

Proposition 21 *Let F be an algebraic field extension of K and $v : K \longmapsto \mathbf{Z}$ the trivial valuation on K. Then an extension of v to F is trivial.*

PROOF Let $x \in F^*$. As F is algebraic over K, we may write

$$a_0 + a_1 x + \cdots + a_n x^n = 0,$$

with the $a_i \in K \setminus \{0\}$. The number of i nonzero is greater or equal to 2, since x is algebraic and nonzero. We may now apply Corollary 4 to the sum of the $a_i x_i$ and deduce that there exist $1 \leq i < j \leq n$ such that $v(a_i x^i) = v(a_j x^j)$, i.e.,

$$v(a_i) + iv(x) = v(a_j) + jv(x) \Longrightarrow v(x) = -\frac{v(a_j) - v(a_i)}{j - i}.$$

As $a_i, a_j \in K^*$, we have $v(x) = 0$. □

Remark Let F be a field and V a DVR in F, with associated discrete valuation v. If K is a field included in V, then v is trivial on K, so F cannot be an algebraic extension of K. However, if F is not an algebraic extension of K, then a DVR in F may contain the field K. Here is an example. Consider the case where K is a field and $F = K(X)$; then F is not an algebraic extension of K. If, for $\frac{f}{g} \in F^*$, we set $v(\frac{f}{g}) = \deg f - \deg g$, and $v(0) = +\infty$, then v is a discrete valuation on F and its valuation ring V is composed of the rational fractions $\frac{f}{g}$ such that $\deg f \geq \deg g$. Clearly $K \subset V$.

Corollary 11 *If F is a finite extension of the field K and V is a DVR in F, then $V' = K \cap V$ is a DVR in K. In addition, V' is the only DVR in K contained in V.*

PROOF Let $v : F \longrightarrow \mathbf{Z}$ be the discrete valuation associated to V. From Proposition 21, the restriction of v to K is not trivial. Thus the image of v restricted to K^* is a nonzero ideal (k) in $\mathbf{Z}$. We may suppose that $k > 0$. Then

$$V' = V \cap K = \{x \in K : v(x) \geq 0\} = \{x \in K^* : v'(x) \geq 0\} \cup \{0\}.$$

where $v' = \frac{1}{k} v$. Given that v' is a surjective mapping from K^* onto $\mathbf{Z}$, v' is a discrete valuation and V' is a DVR in K, as claimed.

Suppose now that U' is a DVR in K and $U' \subset V$. Then $U' \subset K \cap V = V'$. From Corollary 6, we have $U' = V'$. So V' is the unique DVR in K contained in V □

In the next result we show that if V' is a DVR in a field K and F is a finite extension of K, then we may extend V' to a DVR in F.

Proposition 22 *Let F/K be a finite separable field extension. If V is a DVR in K, then there is a DVR W in F such that $W \cap K = V$. The number of such DVRs W is finite.*

PROOF Let C be the integral closure of V in F. From Proposition 18, C is a Dedekind domain with a finite number of nonzero maximal ideals. Let us fix a maximal ideal Q. The localization C_Q is a DVR and $R = C_Q \cap K$ is a ring containing V and included in K. If $V \neq R$, then there exists $x \in R$ such that $v(x) < 0$, where v is the discrete valuation on K whose valuation ring is V. Let t be a uniformizer of V. Then there exists a unit u in V such that $x = ut^n$, for some $n < 0$. Multiplying x by $u^{-1}t^{-n-1}$, which belongs to V and hence to R, we obtain t^{-1}. Thus $t^{-1} \in R$ and it follows that $R = K$. However, this is impossible as we will now see.

Let P be the unique maximal ideal of V. As K is the fraction field of V, for any $b \in P^*$, we have $b^{-1} \in K$. Moreover, $b^{-1} \notin C_Q$: as $P^* \subset Q$, we have $b \in Q$, which implies that $b^{-1} \notin C_Q$. It follows that $K \neq R$. Thus we have at least k DVRs W in F such that $W \cap K = V$, where k is the number of maximal ideals in the decomposition of C into maximal ideals. In fact, there are just k DVRs W in F such that $W \cap K = V$, which we will now show.

Suppose that W is a DVR in F such that $W \cap K = V$, then W has a unique maximal ideal Q'. If $x \in C$, then x is an element of F which is a zero of a monic polynomial with coefficients in V. However, V is included in W, so x is a zero of a monic polynomial with coefficients in W. As W is integrally closed, we have $x \in W$. Hence C is included in W.

Let $Q = C \cap Q'$. Then Q is a prime ideal in C. ($Q \neq C$, because in this case $1 \in Q \subset Q'$, which is impossible.) Also, $Q \neq \{0\}$: First, WP is an ideal in W and so is included in a maximal ideal. As Q' is the unique maximal ideal in W, we have $P \subset Q'$. Also, as $P \subset V$, necessarily $P \subset C$, so $P \subset C \cap Q' = Q$. Hence $Q \neq \{0\}$, as claimed.

We aim to show that $W = C_Q$. A simple verification shows that $C_Q \subset W_{Q'}$. If $x \in W_{Q'}$, then $x = \frac{r}{s}$, with $r \in W$ and $s \in W \setminus Q'$. However, if $s \in W \setminus Q'$, then s is a unit in W and so x is the product of two elements of W and hence lies in W. Therefore $W_{Q'} \subset W$. Thus $C_Q \subset W$. Now, applying Corollary 6, we obtain $C_Q = W$, as required. □

In the remark after Corollary 5 we observed that there is a bijection from the discrete valuations on F onto the discrete valuation rings contained in F. In this section we consider the case where K is a subfield of F. We note $\mathcal{V}(F/K)$ the set of discrete valuations v on F such that $v(x) = 0$, for all $x \in K^*$ and $\mathcal{D}(F/K)$ the set of discrete valuation rings V with $K \subset V \subset F$. From Proposition 21, if F is an algebraic extension of K, then the two sets $\mathcal{V}(F/K)$ and $\mathcal{D}(F/K)$ are empty, because there can be no nontrivial valuation on F. We will exclude this case.

Proposition 23 *The mapping ϕ sending a discrete valuation on F to its valuation ring is a bijection from $\mathcal{V}(F/K)$ onto $\mathcal{D}(F/K)$.*

PROOF If $v \in \mathcal{V}(F/K)$ and $x \in K^*$, then $v(x) = 0$ and so $K^* \subset V$, the valuation ring associated to v. As $0 \in V$, we have $K \subset V$. Therefore the image of $\mathcal{V}(F/K)$ under ϕ is contained in $\mathcal{D}(F/K)$. From Corollary 5 the mapping ϕ is injective.

Now suppose that $V \in \mathcal{D}(F/K)$ and let v be the discrete valuation on F whose valuation ring is V. Since K is a field, an element $x \in K^*$ is invertible and so $v(x) = 0$. This implies that $v \in \mathcal{V}(F/K)$. It follows that ϕ maps $\mathcal{V}(F/K)$ onto $\mathcal{D}(F/K)$. □

Here is an example. Let K be a field and $D = K[X]$. The fact that D is a PID implies that D is a Dedekind domain. Clearly K is contained in D and $F = K(X)$ is the fraction field of D. Now let P be a nonzero prime ideal in D. Then the localization D_P is a DVR containing D, hence K, and the fraction field of D_P is that of D, namely F. Hence $D_P \in \mathcal{D}(F/K)$. From Proposition 23, there is a unique element $v \in \mathcal{V}(F/K)$, such that $\phi(v) = D_P$. We aim to find v.

We consider the P-adic valuation v_P. The valuation ring of v_P is D_P and v_P vanishes on $D \setminus P$. If $x \in K^*$, then x is invertible and so $x \in D \setminus P$, hence $v_P(x) = 0$. Thus v_P is the element

$v \in \mathcal{V}(F/K)$ we were looking for.